No. 17-2

In The
Supreme Court Of The United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

On Writ of Certiorari to the United States
Court of Appeals for the Second Circuit

BRIEF FOR 51 COMPUTER SCIENTISTS AS AMICI CURIAE IN SUPPORT OF THE RESPONDENT

John D. Vandenberg
Counsel of Record
Klaus H. Hamm
KLARQUIST SPARKMAN, LLP
121 SW Salmon St., Ste. 1600
Portland, OR 97204
503-595-5300
john.vandenberg@klarquist.com

Attorneys for the Amici Curiae

January 17, 2018

TABLE OF CONTENTS

INTEREST OF THE AMICI 1

SUMMARY OF ARGUMENT 7

ARGUMENT 9

I. "CLOUD" DATA ALWAYS HAS A SPECIFIC PHYSICAL LOCATION 9

II. RETRIEVING DATA FROM A "CLOUD" DATACENTER IN IRELAND REQUIRES COMPLEX PHYSICAL ACTIONS IN IRELAND 16

III. THE DATA IS PROTECTED IN A DIGITAL SAFE DEPOSIT BOX 25

IV. THE CLOSER THE DATA, THE FASTER THE ACCESS 29

CONCLUSION 30

TABLE OF AUTHORITIES

CASES

Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) 18

OTHER AUTHORITIES

Brendon Lynch, *Your Email Belongs to You, Not Us*, Microsoft Secure Blog (Aug. 27, 2014), https://cloudblogs.microsoft.com/microsoftsecure/2014/08/27/your-email-belongs-to-you-not-us/ 28

Eric Griffith, *What Is Cloud Computing?*, PC Mag. (May 3, 2016), http://www.pcmag.com/article2/0,2817,2372163,00.asp 10

Federal Information Processing Standard (FIPS) 197, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. 28

Jelle Frank Van Der Zwet, *Layers of Latency: Cloud Complexity and Performance*, Wired (Sept. 18, 2012), http://www.wired.com/2012/09/layers-of-latency/ 30

Matt Thomlinson, *Advancing Our Encryption and Transparency Efforts*, Microsoft on the Issues (July 1, 2014), http://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/ 29

Microsoft, *Cloud Operations Excellence & Reliability* 5 (2014), http://download.microsoft.com/download/E/3/0/E30B17E4-E70D-41E3-83E1-C22B767A76BC/Cloud_Operations_Excellence_Reliability_Strategy_Brief.pdf 26

Microsoft, *Cloud-Scale Datacenters* 2 (2014), http://download.microsoft.com/download/B/9/3/B93FCE14-50A2-40F6-86EE-8C1E1F0D3A95/Cloud_Scale_Datacenters_Strategy_Brief.pdf.....12

Microsoft Datacenters, http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx 12

Microsoft Datacenters, *Microsoft Datacenter Tour (long version)*, https://youtu.be/0uRR72b_qvc.....12

Microsoft, *How Microsoft Designs Its Cloud-Scale Servers* 4 (2014), http://download.microsoft.com/download/5/7/6/576F498A-2031-4F35-A156-BF8DB1ED3452/How_MS_designs_its_cloud_scale_servers_strategy_paper.pdf 21

Microsoft, *Information Security Management System for Microsoft's Cloud Infrastructure* 1 (2015), http://download.microsoft.com/download/A/0/3/A03FD8F0-6106-4E64-BB26-13C87203A763/Information_Security_Management_System_for_Microsofts_Cloud_Infrastructure.pdf 26

Microsoft, *Protecting Data and Privacy in the Cloud* 8 (2014), http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf 27

Microsoft, *Securing the Microsoft Cloud Strategy Brief* 5 (2015), https://download.microsoft.com/download/D/5/E/D5E0E59E-B8BC-4D08-B222-8BE36B233508/Securing_Microsoft_Cloud_Strategy_Brief_.pdf 27

Microsoft's Quest for Greater Efficiency in the Cloud (Apr. 19, 2011), http://news.microsoft.com/2011/04/19/microsofts-quest-for-greater-efficiency-in-the-cloud/ 12

Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication No. 800-145 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. 10

Quentin Hardy, *Bearing Down On Data Upstarts*, THE NEW YORK TIMES, Aug. 24, 2014, https://www.nytimes.com/2014/08/25/technology/box-dropbox-and-hightail-pivot-to-new-business-models.html 13

Stephan Somogyi, *Making End-to-End Encryption Easier to Use*, Google Security Blog (June 3, 2014), http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html 29

Transport Layer Security, RFC 5246, Internet Engineering Task Force, https://tools.ietf.org/html/rfc5246 18

INTEREST OF THE AMICI[1]

The 51 amici identified below are computer and data science experts. Amici have an interest in ensuring that the intersection between law and technology reflects an accurate awareness of the technology at issue and its real-life implementations. As professors who routinely research and teach computer science concepts, amici are well-positioned to provide a firm technological foundation for the resolution of the important legal disputes of this case regarding the storing and accessing of electronic data.

Amici are leading researchers in computer systems, networking, distributed systems, computer security, cryptography, and computer architecture—the foundations of "cloud" computing. They include members of the National Academy of Engineering and the National Academy of Sciences; winners of the Turing Award (the "Nobel Prize" of computer science); and Fellows of the American Academy of Arts & Sciences, the Association for Computing Machinery, the Institute of Electrical and Electronics Engineers, and the American Association for the Advancement of Science. While many have industry experience, all are now faculty members at leading computer science programs, including at Brown, Boston University,

---

[1] The parties have consented to the filing of this brief in letters of consent on file with the Clerk. No counsel for any party authored this brief in whole or in part, and no party or counsel for any party provided any monetary contribution to its preparation or submission.

Brigham Young, Carnegie Mellon, Columbia, Cornell, Duke, Harvard, Johns Hopkins, MIT, New York University, Portland State, Princeton, Purdue, Rice, Stanford, Toyota Technological Institute at Chicago, University of California at Berkeley, University of California at Davis, University of California at Santa Cruz, University of Edinburgh, University of Maryland, University of Massachusetts Amherst, University of Michigan, University of North Carolina at Chapel Hill, University of Pennsylvania, and University of Washington.

A list of amici appears below. Amici are signing this brief on their own individual behalf and not on behalf of any company, university, or other organization with which they are affiliated.

Azer Bestavros, Computer Science Department, Boston University

Matt Bishop, Department of Computer Science, University of California at Davis

Matthew Blaze, Department of Computer and Information Science, University of Pennsylvania

Avrim L. Blum, Toyota Technological Institute at Chicago

Dan Boneh, School of Engineering, Stanford University

Eric A. Brewer, Electrical Engineering and Computer Sciences Department, University of California at Berkeley

Frederick P. Brooks, Jr., Department of Computer Science, University of North Carolina at Chapel Hill

Douglas E. Comer, Computer Science Department, Purdue University

Fernando Corbato, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

David J. Farber, Department of Computer Science and Public Policy, Carnegie Mellon University

Nick Feamster, Computer Science Department, Princeton University

Edward Feigenbaum, Computer Science Department, Stanford University

Michael J. Freedman, Department of Computer Science, Princeton University

Allan Gottlieb, Computer Science Department, Courant Institute, New York University

John Guttag, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

J. Alex Halderman, Department of Electrical Engineering and Computer Science, University of Michigan

Mor Harchol-Baltor, Department of Computer Science, Carnegie Mellon University

Nadia Heninger, Computer and Information Science Department, University of Pennsylvania

John L. Hennessy, Department of Electrical Engineering and Computer Science, Stanford University

Haym B. Hirsh, Department of Computer Science, Cornell University

Daniel Peter Huttenlocher, Department of Computer Science, Cornell University

Brian Kernighan, Department of Computer Science, Princeton University

Jon Kleinberg, Department of Computer Science, Cornell University

Edward D. Lazowska, Paul G. Allen School of Computer Science & Engineering, University of Washington

Henry M. Levy, Paul G. Allen School of Computer Science & Engineering, University of Washington

Barbara Liskov, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Darrell Long, Department of Computer Engineering, University of California at Santa Cruz

Anna Lysyanskaya, Computer Science Department, Brown University

Bruce MacDowell Maggs, Department of Computer Science, Duke University

Kathleen R. McKeown, Department of Computer Science, Columbia University

Nick W. McKeown, Departments of Computer Science and Electrical Engineering, Stanford University

David Maier, Department of Computer Science, Portland State University

John Gregory Morrisett, Faculty of Computing & Information Science, Cornell University

David A. Patterson, Electrical Engineering and Computer Sciences Department, University of California at Berkeley

William W. Pugh, Department of Computer Science, University of Maryland, College Park

Raj Reddy, Department of Computer Science and Robotics, Carnegie Mellon University

Jennifer Rexford, Computer Science Department, Princeton University

Ronald L. Rivest, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Aviel D. Rubin, Department of Computer Science, Johns Hopkins University

Fred B. Schneider, Department of Computer Science, Cornell University

Dana S. Scott, Department of Computer Science, Carnegie Mellon University

Scott Shenker, Electrical Engineering and Computer Sciences Department, University of California at Berkeley

Eugene H. Spafford, Department of Computer Sciences, Purdue University

Ivan E. Sutherland, Department of Electrical Engineering & Computer Science, Portland State University

Michael Stonebraker, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Eva Tardos, Department of Computer Science, Cornell University

Donald F. Towsley, College of Information and Computer Sciences, University of Massachusetts Amherst

Philip Wadler, Department of Theoretical Computer Science, Laboratory for Foundations of Computer Science, School of Informatics, University of Edinburgh

James H. Waldo, Department of Computer Science, Harvard University

Dan S. Wallach, Department of Computer Science, Rice University

Doran K. Wilde, Department of Electrical & Computer Engineering, Brigham Young University

SUMMARY OF ARGUMENT

More than a billion people around the world safeguard their private emails and other data in hundreds of high-security datacenters operated by trusted American "cloud" service providers such as Amazon, Google, IBM, and Microsoft. This new paradigm combines the highest security for one's most personal data with nearly instantaneous access from anywhere in the world.

Like the telegraph, telephone, and Internet before it, the "cloud" is built on old and new technologies. Any legal decisions involving this new paradigm should be based on a clear understanding of the underlying science and engineering. For example, it should not conflate where data is accessible with where it is located. Nor should it overlook the myriad physical actions required at the datacenter to deliver on two of the "cloud's" primary promises: security and speed of access. We hope our brief assists this Court in reaching such an understanding.

We explain the following points based on the underlying computer science of this "cloud" technology and service:

1. The data is at a specific physical location: While the "cloud" allows the owner of personal data to access her data from Internet-connected

computers throughout the world, and to do so without being aware of the location of the data, the data is always stored in at least one specific location: an electronic pattern of digital 0s and 1s on a spinning disk, or similar storage device, in a computer in a datacenter.

2. Retrieving data from Ireland requires complex physical actions in Ireland: Retrieving data stored on a spinning computer disk, or similar device, in a high-security datacenter in Ireland requires myriad complex physical actions in Ireland.

3. The data is protected in a digital "safe deposit box": The owner's personal data is made more secure in a "cloud" datacenter than on most home computers. This includes being shielded, by encryption, from employees of the datacenter to an even greater extent than personal papers in a safe deposit box in a bank vault are protected from a bank's employees. The owner's personal data also is protected in transit to and from the datacenter in a digital equivalent to an armored truck—again by means of encryption.

4. The closer the data, the faster the access: Geography matters, as the data owner's rapid access to her personal data is faster if the data is stored at the "cloud" service provider's nearest regional datacenter.

ARGUMENT

I. "CLOUD" DATA ALWAYS HAS A SPECIFIC PHYSICAL LOCATION.

A long-distance telephone call may be so clear that it sounds as if the other person is in the next room, even if she is hundreds or thousands of miles away. This is not because she speaks differently than her ancestors 150 years ago, of course, but because technology (the telephone) has changed, making her speech accessible remotely. She is present in one place but can be heard virtually everywhere.

Something similar is true of one's personal private data (e.g., private emails, photos, etc.) stored hundreds of miles away in a cloud datacenter. It can be accessed so rapidly that it seems to be present in the computer, tablet or smart phone one is touching. The data itself has not changed from that stored on computers 50 years ago. Nor has the basic science for using magnetic fields to store data inside a computer. But thanks first to the Internet and now to the "cloud," such data stored far away can be accessed so rapidly that it seems to be inside the computer, tablet or smart phone on or in the desk, hands, or lap of the person accessing it. The data is physically present in one place but can be accessed virtually anywhere.

That data at one physical location can be privately accessed from virtually unlimited locations by its owner, almost instantly, is at the heart of "cloud" services. It means that the data can be stored in special high-security datacenters with the latest security technology to ensure the data's

confidentiality, yet be instantly (almost) and privately accessed by its owner from anywhere (almost) and thus appear to be everywhere—"in the cloud."

What do we mean by "data"? Computing revolves around *binary* data—vast quantities of 0s and 1s (called bits for "binary digits") stored on a physical drive that collectively represent the photos, letters, spreadsheets, emails, and everything else we use computers to store, view, edit, and share. The advent of "cloud" computing has transformed how we interact with that data. No longer must we be in the same room with our private data to read it, tied to specific computers and physical storage devices. Instead, "the cloud" enables us to retrieve data from—and share it with—any device with an Internet connection. Thus, while "cloud" computing has been defined, by the government for example, as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction,"[2] the basic concept is actually quite simple—"cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive."[3]

---

[2] Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication No. 800-145, at 2 (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[3] Eric Griffith, *What Is Cloud Computing?*, PC Mag. (May 3, 2016), *available at* http://www.pcmag.com/article2/0,2817,2372163,00.asp.

Following decades of primarily local data storage, the meteoric rise of highly secured "cloud" datacenters from the likes of Amazon, Google, IBM, and Microsoft has happened over the past 10 years. Before the "cloud," people primarily stored data locally. Whether located on a corporate mainframe computer, on a personal computer, or on portable storage devices that can be read by a computer (such as a USB "thumb drive" or a disc such as a CD-ROM), people have stored (and in many cases continue to store) their data on local, physical media. For example, someone might draft a document using word processing software installed on her laptop computer and then save the document to the internal hard drive of the computer, a shared company server, or a portable drive. The devices that store data have evolved from large sets of unwieldy "floppy disks" prone to decay and slow to store or retrieve data to fast, modern, solid-state storage devices that can fit on a keychain, have no moving parts, cost less than a fast-food meal, and have the capacity of thousands of archaic floppy disks. But, still one had to be in the same location as the data to access it.

Corporate data storage has likewise evolved, with modern data servers consistently becoming smaller, faster, more efficient, and capable of storing immense amounts of data. These data servers traditionally housed the important files and communications of an entire company in an on-site server room or datacenter. Yet all of these devices relate to an increasingly outmoded paradigm—local data storage and retrieval. One still had to be in the same building, or at least connected to the same corporate network, as one's data.

At the dawn of the telephone, some who first heard a distant friend's voice over the telephone must for a moment have thought that the friend was in the next room. Today, with this new paradigm of "cloud" computing, some similarly conflate where data is located with where it can be accessed. But, the ability to almost instantly access data "in the cloud" from almost anywhere does not mean that the data follows its owner around the world. Instead, no matter where it is accessed at any given instant, all data stored "in the cloud" has at least one identifiable physical location. Each private email, for example, is stored on at least one specific item of physical media one could touch, typically on a specific spinning magnetic "hard disk" in a specific, special, highly secured "server" computer inside a high-security datacenter such as Microsoft's facility in Dublin, Ireland pictured below.[4]

---

[4] Image from Microsoft, *Microsoft's Quest for Greater Efficiency in the Cloud* (Apr. 19, 2011), *available at* http://news.microsoft.com/2011/04/19/microsofts-quest-for-greater-efficiency-in-the-cloud/; *see also* Microsoft, *Cloud-Scale Datacenters* 2 (2014), *available at* http://download.microsoft.com/download/B/9/3/B93FCE14-50A2-40F6-86EE-8C1E1F0D3A95/Cloud_Scale_Datacenters_Strategy_Brief.pdf (noting that Microsoft "has invested over $15 billion in building a highly scalable, reliable, secure, and efficient globally distributed datacenter infrastructure"). Additional information regarding Microsoft's datacenters, including a short video, is also available at: http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx; *see also* Microsoft Datacenters, *Microsoft Datacenter Tour (long version)*, *available at* https://youtu.be/0uRR72b_qvc (noting that Microsoft's cloud platform "infrastructure is comprised of a large global portfolio of more than 100 datacenters, 1 million servers, content distribution networks, edge computing nodes, and fiber optic networks").

These datacenters house thousands of server computers, all physically linked together as shown in the picture below to provide secure, reliable, and efficient data access.[5]

---

[5] Image from Quentin Hardy, *Bearing Down On Data Upstarts*, THE NEW YORK TIMES, Aug. 24, 2014, *available at* https://www.nytimes.com/2014/08/25/technology/box-dropbox-and-hightail-pivot-to-new-business-models.html.

American companies—Amazon, Google, IBM, and Microsoft—currently operate the vast majority of such "cloud" datacenters in the world. Unlike datacenters devoted to a single corporation's data, these "cloud" service providers make their datacenters available to anyone to store private data with the assurance that such data shall remain private. They provide, in essence, highly secure bank-vault safe deposit boxes for safeguarding personal data—accessible 24/7 privately, almost instantly, almost anywhere in the world.

Most email in such datacenters is stored in basically the same way most computer data has been stored since IBM invented "hard disks" in the 1950s: using magnetic fields inside the computer storage media.

(Before magnetic storage of data, the primary computer data storage medium was a paper card with punched holes to represent 1s and 0s. American inventor Herman Hollerith invented a punch card tabulating machine able to complete the 1890 Census

in one year versus the eight years it took to hand tabulate the 1880 census. Punch cards were used in computing through the late 1970s and for elections even later, causing the infamous "hanging chads" conundrum.)

Hard disks and similar storage devices record data using basic electromagnetic principles. Each spinning disk (called a "hard disk" to distinguish from old "floppy disks"), consists of some solid substrate (e.g., aluminum) coated with a film of magnetizable material (e.g., iron oxide). This film contains individual magnetic particles arrayed in random directions—unless subjected to a magnetic field. When subjected to a magnetic field, these magnets turn to align in a direction dictated by the polarity of that magnetic field. This physical property is used to turn these magnets, at predefined positions on the disk, into one of two different directions. Each sequential change in direction of magnetization represents one of two binary values, representing true or false or 1 or 0, akin to the presence or absence of a hole in a punch card. A series of magnetic direction changes may represent a series of these 1s and 0s, which in turn represent a character (e.g., the letter "a") or a number. For example, the number 15 typically is represented by magnetic direction changes in the magnetic film representing the following series of 1s and 0s: 00001111.

Each sequence of magnets has, of course, a single identifiable physical location, as much so as a punch card with holes signifying "15" or lines of chalk on a blackboard representing the number 15. Even though that number 15 on the punch card or blackboard can

be quickly accessed around the world (e.g., being read over a long-distance telephone call), the data itself is at one identifiable physical location.

In sum, the "cloud" is merely the latest iteration of an information-access evolution, which started with couriers, followed by the telegraph, facsimile, telephone, and most recently the Internet. However, the data being accessed is still located at a specific identifiable location, as is the friend on the long-distance phone call.

II. RETRIEVING DATA FROM A "CLOUD" DATACENTER IN IRELAND REQUIRES COMPLEX PHYSICAL ACTIONS IN IRELAND.

It is impossible to retrieve data from a high security datacenter in Ireland without complex physical actions occurring in Ireland. While most of these actions occur at a microscopic level, they are no less physical or necessary than if the same data were protected in a bank-vault safe deposit box in a Dublin bank.

Assume a Dublin bank employee received a telephone call from the New York office telling her that a New York court had ordered her to open a customer's safe deposit box in the bank vault and send copies of all papers in it to New York. The bank employee in Dublin may need to at least (1) search for and find the branch's secured master key; (2) search for and find the correct safe deposit box; (3) use her master key in the box's first lock; (4) have a locksmith pick the box's second lock (normally opened by the

owner's key); (5) remove the papers from the box; (6) make copies of the papers; (7) put the copies into an envelope; (8) apply sealing wax to the envelope; (9) stamp the sealing wax with the custom bank stamp; (10) put the sealed envelope into a locked attaché case per the bank's security protocols; and (11) hand the locked case to a trusted bank courier to fly it to the New York office.

Comparable physical actions must be taken by an Irish datacenter when a copy of a customer's personal emails is requested from the United States. Just as many of the above steps by the Dublin bank are required by security mechanisms protecting the privacy of the customer's personal data, most of the physical actions at the datacenter when data is retrieved are required by security mechanisms protecting the privacy of the customer's personal data.

The Brief for the United States states that "Microsoft could comply with the warrant by undertaking acts entirely within the United States." (Brief at 25). This parallels Judge Lynch's remark that "the entire process of compliance takes place domestically." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 229 (2d Cir. 2016) (Lynch, J., concurring). To the extent that these statements imply that it is possible for someone in the United States to search for, copy, transmit, and disclose data stored in a datacenter in Ireland, without any physical actions happening at that datacenter, the statements are incorrect. It would be as inaccurate as saying that a bank can retrieve copies of personal papers in a safe

deposit box in Dublin "by undertaking acts entirely within the United States."

When the owner of personal data requests her data from the "cloud" service provider, and the data is stored at a datacenter in Ireland, the physical actions set out below must occur in Ireland. This is equally true when anyone else requests that data, such as special personnel of the "cloud" service provider accessing the data to comply with a court order.

The physical actions listed below typically are taken using multiple computer chips, including a "central processing unit" (CPU)—commonly referred to as the "brains" of a computer—and a "random access memory" (RAM) chip—equivalent to a brain's short-term memory. Collectively, these actions may involve millions of machine operations by the computer's processor, in Ireland, guided by millions of lines of computer code stored and executed on computers in Ireland.

1. Implement secured communications protocols to verify the request: Communications between the data requester and the datacenter are encrypted and secured, for example by the Transport Layer Security (TLS) protocol.[6] Computers at the datacenter in Ireland must take actions required by this protocol when receiving and verifying the data request from the United States. (This is somewhat akin to the Dublin bank employee asking a series of

[6] The current TLS protocol is a standard defined in RFC 5246 by the Internet Engineering Task Force, and available at https://tools.ietf.org/html/rfc5246.

questions of the New York office requester, who must provide the correct secret answers for the branch to accept the request.) The datacenter must then use the correct decryption keys to decrypt the request, i.e., to decode the message from the gibberish created and stored by the original encryption process.

2. Authenticate the data requester: The computers at the datacenter must take actions to verify that the person who sends the request for the owner's data actually is the owner (or the service provider officer). Typically, this includes verifying that the requester has provided a recognized username and the correct password associated with that username, but often requires more "authentication" security checks. For example, one type of "two-factor authentication" also requires the user to promptly respond to a notification texted to the user's smart phone, so that a hacker who found the user's password could not access her private emails unless he also had stolen her smart phone and its password. (This is somewhat akin to a bank employee requiring photo identification—in addition to presentation of the key—from a customer seeking to access a safe deposit box.)

3. Enforce access controls: Just as few would store their most personal letters in their local library's reading room, few would trust their personal emails with "cloud" service providers if others could easily read that personal data. Therefore, the "cloud" datacenter strictly

restricts who can access that data and under what limited circumstances—exactly as a bank would limit who can have the keys needed to open the bank-vault safe deposit box and under what circumstances.

This is enforced in part through "access controls" imposed on the data. Among other things, this prevents employees from Amazon, Google, IBM, or Microsoft, or the Government, from accessing and reading the emails of anyone who entrusts their personal data to "the cloud." There are many access control enforcement mechanisms, including "just-in-time" access control where no one other than the owner has default access to the data, not even any legal department personnel for the service provider. Instead, people other than the owner must request short-term access rights on an as-needed basis. Before any personal data is read from a spinning magnetic disk, the computer's CPU and memory chip perform the actions needed to securely enforce these access control restrictions. (This is somewhat similar to a bank confirming that a person presenting an identification is listed as the person who has permission to access a safe deposit box.)

4. Read and process the accepted request: Once the computer in Ireland has decrypted and verified the request, authenticated the requester, and enforced all applicable access controls, the computer must take physical actions to read and "understand" the request, and ascertain what data it is requesting (e.g.,

which email or other personal data of which customer, etc.).

5. Search for the requested data: When the bank's New York office calls the Dublin branch, the caller may not know the precise number or location of the bank-vault safe deposit box of the personal papers he requests. Instead, the local branch controls and knows which safe deposit boxes are assigned to which customers. Similarly, in "cloud datacenters," the data's requester does not know which portion of which spinning disk stores the data. Rather, many actions at the datacenter are needed to search for the physical location of the requested data. The datacenter computers use "database management system" software to organize information about the data they store (e.g., file names, dates, file size, location of the data in physical storage, etc.) in a structured database. Among other things, this contains information permitting the datacenter computer to store and retrieve the underlying data from the computer's "file management system," which in turn ultimately stores the data as 1s and 0s on magnetic or solid-state storage drives within the datacenter computers.[7]

---

[7] *See, e.g.*, Microsoft, *How Microsoft Designs Its Cloud-Scale Servers* 4 (2014) (describing the hard drives utilized in Microsoft's servers), *available at* http://download.microsoft.com/download/5/7/6/576F498A-2031-4F35-A156-BF8DB1ED3452/How_MS_designs_its_cloud_scale_servers_strategy_paper.pdf.

6. Read the data from the spinning hard disk: Retrieving data from storage media (e.g., a spinning hard disk) is called "reading" the data. Reading data from a spinning disk is a complicated physical action inside the datacenter computer. To be able to associate particular magnetic field patterns with particular information, each spinning disk includes magnetic markers organizing the disk into different storage regions. Special data stored on the disk identifies which regions store what data. This special data, like a map, may indicate that the requested email begins at a specific cluster on the disk. Special read/write heads of the "hard disk drive" must be moved into the precise correct position to read this map to find the location of the desired data on the disk. Once the data is located on the disk, then the read/write heads are physically moved into position over the spinning disk to detect (read) the magnetic fields representing the data. Changes in direction of the magnetic fields generate electrical signals in the read/write head that are interpreted as the 1s and 0s representing the data. The remote requester (e.g., in the United States) will never know the actual physical location of the data (e.g., what cluster on what disk drive of what computer stored the email message).

7. Copy the data to short-term memory: Once the requested data is read, it then is copied into a particular portion of short-term memory in a RAM chip at the datacenter. This RAM chip uses different technology for storing data. This

RAM is a computer chip, not a spinning disk. It uses electrical pulses in microscopic electronic switches (i.e., transistors) and other electronic devices, to store the data. This chip stores less information than spinning disks, and for only short periods, but it has no physical moving parts and thus can access and copy data more quickly than the spinning disks and moving read/write heads of a hard disk drive. Although the mechanisms are different, storing data in RAM likewise requires many physical actions inside the computer. (This is similar to a bank employee copying paper documents removed from a safe deposit box.)

8. Encrypt and package the data for transmission over the Internet: Before this data copied into the RAM memory chip can be transmitted away from the datacenter, it needs to be packaged according to multiple protocols—that is, sets of rules that govern how data is formatted and transmitted from one physical location to another in a secure, efficient, and reliable way. Some of this data packaging "encrypts" the data to maintain its secrecy in transit. Anyone who intercepts the data transmission will be able to read only gibberish if the interceptor does not have the correct decryption key. For example, rather than transmit the number 15 as 00001111, the datacenter might encode that as 10110001, and only someone with the correct decryption key would be able to decode that back into the correct value 00001111. (This is similar to a bank employee placing copies of a document in a secure container for transit.)

The above descriptions merely skim the surface of the actions that occur inside a datacenter's computer when a request to retrieve a customer's personal data is received. Scores of computer science courses at amici's institutions are devoted to these topics. What is important here is that when data is requested from a datacenter in Ireland, the above and more actions necessarily must occur and do occur in Ireland to decrypt the request, authenticate the requester, confirm the requestor's authority to make the request, find the data, read and copy the data, and protect the data before it is released.

These necessary and fundamental actions occur in Ireland as surely as a bank employee in Dublin acts in Ireland when ordered to abide by all security protections before she enters the bank's vault, opens a customer's safe deposit box, copies a private letter lying in the box, and hands a copy to a courier to bring the copy to the New York office.

While no human can act quickly enough to perform the physical actions required in the datacenter, that makes them no less physical and no less clearly located in Ireland. Humans are, of course, required by the "cloud" provider to be present at the datacenter in Ireland, however, to maintain the security and operational integrity of the datacenter. Similarly, if the datacenter in Ireland had a complete failure of its power system or was disconnected from the Internet, there would be no way to access the data stored there by an operator located in the United States. But the data would still be present in Ireland.

In sum, when data is retrieved from a datacenter in Ireland, the most important actions occur in Ireland, from the perspective of the fundamental promises of "cloud" computing: security (of the private data) and speed (of access by the rightful owner).

III. THE DATA IS PROTECTED IN A DIGITAL SAFE DEPOSIT BOX.

For more than 150 years, people have trusted bank-vault safe deposit boxes to safeguard their valuable personal property. They trust that their private papers will remain private, and not be accessed by bank employees or others. And they know that the bank can afford armed guards, thick-walled vaults, and other security measures they cannot. The banks, in turn, know that this business of safeguarding customers' private assets depends on honoring their promise of providing the highest security.

"Cloud" service providers are high-tech versions of banks providing bank-vault safe deposit boxes. They can afford the best possible security, and they know their business depends on keeping private their customers' personal data. Therefore, every email stored in "the cloud" is safeguarded as it would if stored in a bank vault's safe deposit box, possibly more so.

Digital security of "cloud" emails has many more levels and sophistication than any bank-vault safe deposit box, requiring more keys to access the contents. These keys and security systems are largely transparent to the user, but users expect that before

anyone can read or copy a customer's stored email message, including anyone working at Google, Apple, or Microsoft, many high-security digitally locked doors must be unlocked.

Datacenters routinely secure their customer's data with advanced physical and electronic safeguards, access controls, and other technological security measures to prevent unauthorized access.[8] Storing data "in the cloud" averts the risk of data loss, as the data is no longer stored on one's personal devices, but rather in physically secure datacenters, which employ built-in redundancies (e.g., copies on multiple hard drives) to ensure against hardware failures and physical damage.[9]

Although safeguarded by the "cloud" service provider, an individual customer's email content is

---

[8] *See, e.g.*, Microsoft, *Information Security Management System for Microsoft's Cloud Infrastructure* 1 (2015), *available at* http://download.microsoft.com/download/A/0/3/A03FD8F0-6106-4E64-BB26-13C87203A763/Information_Security_Management_System_for_Microsofts_Cloud_Infrastructure.pdf (including "an overview of the key certifications and attestations Microsoft maintains to demonstrate to cloud customers that information security is central to Microsoft's cloud operations").

[9] *See, e.g.*, Microsoft, *Cloud Operations Excellence & Reliability* 5 (2014), *available at* http://download.microsoft.com/download/E/3/0/E30B17E4-E70D-41E3-83E1-C22B767A76BC/Cloud_Operations_Excellence_Reliability_Strategy_Brief.pdf (noting that "[i]n the event of a natural disaster or service outage, we have programs, procedures, engineers, and operations experts in place to contain issues or rapidly recover with minimal impact on your organization").

considered her private property.[10] As such, email providers typically employ significant security measures to ensure that only those authorized to access the email account may read, edit, copy, or delete the contents of stored messages. For example, login systems ensure that only authorized parties may access an electronic mailbox. And datacenters typically employ dozens of additional security measures including facility security, firewalls, intrusion detection systems, and many others.[11] These extensive security efforts comport with email providers' stated conviction that, "[w]e believe your email belongs to you, not us, and that it should receive

---

[10] *See, e.g.*, Microsoft, *Protecting Data and Privacy in the Cloud* 8 (2014), http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf ("Microsoft believes that its customers should control their own information whether stored on their premises or in a cloud service. Accordingly, we will not disclose Customer Data to a third party . . . except as customers direct or required by law.").

[11] *See, e.g.*, Microsoft, *Securing the Microsoft Cloud Strategy Brief* 5 (2015), *available at* https://download.microsoft.com/download/D/5/E/D5E0E59E-B8BC-4D08-B222-8BE36B233508/Securing_Microsoft_Cloud_Strategy_Brief_.pdf ("When we deploy a service to our datacenters, we assess and address every part of the service stack – from the physical controls, to encrypting all data that moves over our network, to locking down the host servers, to keeping malware protection up-to-date, to ensuring applications themselves have appropriate safeguards in place.").

the same privacy protection as paper letters sent by mail–no matter where it is stored."[12]

The data's security sometimes is enhanced by encrypting the data as it is stored. This is called "at rest" encryption as distinct from the more common "in transit" encryption. For example, Microsoft Windows Server includes a "Bitlocker" drive encryption mechanism using an AES (Advanced Encryption Standard) encryption algorithm.[13] This feature encrypts the data stored on a spinning hard disk. This means that if someone in Ireland successfully broke into a datacenter and found a physical computer having a drive storing a particular email of a particular customer, they could not read that email unless they also had the decryption key. This is another example of extra layers of data security found at "cloud" datacenters that would be unusual in one's home computer.

"Cloud" datacenters do more than protect the customer's data while secured in a digital safe deposit box inside the datacenter. "Cloud" datacenters ensure that the owner's personal data also is protected in transit to and from the regional datacenter, somewhat akin to an armored delivery truck. Email data typically is encrypted or otherwise protected during

---

[12] Brendon Lynch, *Your Email Belongs to You, Not Us*, Microsoft Secure Blog (Aug. 27, 2014), https://cloudblogs.microsoft.com/microsoftsecure/2014/08/27/your-email-belongs-to-you-not-us/.

[13] AES is an internationally recognized standard, available as Federal Information Processing Standard (FIPS) 197 at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

transmission over the Internet, which prevents unauthorized parties from utilizing the data, even if it is intercepted in transit.[14] "Encrypting" the data means that even if someone could access the data in transit, it would be gibberish if they did not also possess the correct decryption key.

IV. THE CLOSER THE DATA, THE FASTER THE ACCESS.

Today, most personal and business mail is email, and most personal (and increasingly business) email is "cloud"-based email. "Cloud" email service providers include Google (Gmail), Yahoo! (Yahoo! Mail), Apple (iCloud), and Microsoft (Exchange Online). Each enables customers to choose to save mail she sends or receives, in the digital equivalent of a bank-vault safe deposit box in the "cloud," and later access it almost instantaneously. But people will not use the "cloud" to store their emails if it takes too long to retrieve them.

---

[14] *See, e.g.*, Matt Thomlinson, *Advancing Our Encryption and Transparency Efforts*, Microsoft on the Issues (July 1, 2014), http://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/ (noting that "when you send an email to someone, your email is encrypted and thus better protected as it travels between Microsoft and other email providers"); Stephan Somogyi, *Making End-to-End Encryption Easier to Use*, Google Security Blog (June 3, 2014), http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html (noting that Gmail "now always uses an encrypted connection when you check or send email in your browser" and discussing a new tool providing "'end-to-end' encryption," which allows "data leaving your browser [to] be encrypted until the message's intended recipient decrypts it").

Although the Internet is very fast, it is slower than the speed of light, and thus geographic considerations are not obviated. To the contrary, choices about where to store data must take "network latency" into account. Latency is the delay between the time data is requested and the time it is delivered. While network latency is often measured in fractions of a second, these seemingly infinitesimal delays have dramatic effects. One study found, for example, "that a half-second delay causes a 20 percent drop in traffic on Google, and a one tenth of a second delay can lower Amazon's sales by 1 percent."[15]

This need to avoid any noticeable delay favors storing the data in the closest datacenter to the customer and in a single datacenter. Retrieving data from multiple datacenters generally involves greater latency (and thus more delay) than from a single datacenter, and requests for data from a nearby datacenter will generally result in significantly less latency (i.e., delay) than requests for data stored on the other side of the globe. Cloud service providers balance latency issues with issues of cost of power, cost of construction and maintenance, labor costs, taxes, locality relative to customers worldwide, and other considerations.

CONCLUSION

Notwithstanding their nearly instantaneous accessibility around the world, personal emails stored in a Dublin cloud datacenter are no less physically

---

[15] Jelle Frank Van Der Zwet, *Layers of Latency: Cloud Complexity and Performance*, Wired (Sept. 18, 2012), *available at* http://www.wired.com/2012/09/layers-of-latency/.

present in Ireland than are personal letters stored in a Dublin bank safe deposit box. Retrieving those emails requires complex physical actions in Dublin just as retrieving those personal letters would, no matter where the person accessing the emails or letters might be located.

Respectfully submitted,

John D. Vandenberg
Counsel of Record
Klaus H. Hamm
KLARQUIST SPARKMAN, LLP
121 SW Salmon St., Ste. 1600
Portland, OR 97204
503-595-5300
john.vandenberg@klarquist.com

Attorneys for the Amici Curiae